

RULES OF BEHAVIOR

The Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources requires that "Rules of Behavior" be established for each general support information technology (IT) system and major application processing government information. The "Rules of Behavior" delineated below pertain to all persons who utilize the Space Network Web Services Interface (SWSI) which is an IT resource of the Mission Services Program Space Network Project of NASA's Goddard Space Flight Center.

As a customer and user of NASA's GSFC IT resources, I understand that I am responsible for adhering to the additional rules listed below:

1. Computer system(s) for which you are requesting or have been issued an account, may only be used for official NASA missions or NASA supported missions.
2. All software on the IT resource is protected in accordance with NASA and Federal Government security and control procedures which will be adhered to.
3. Use of these IT resources gives consent for monitoring and security testing to ensure proper security procedures and appropriate usage are being observed for GSFC Center IT resources.
4. Center IT resources will not be used for fraudulent, harassing or obscene messages and/or materials.
5. Tampering with another user's account, files, data or processes without the other user's express permission, use of the system resources for personal purposes, or other unauthorized activities is strictly prohibited and will result in termination of access privileges.
6. Logon ID's, passwords, and passphrases may never be transferred or shared for any reason.
7. Group ID, group passwords, and group passphrases are prohibited.
8. Passwords:
 - a. will be a minimum of 8 alphanumeric characters;
 - b. will be memorized and not written down;
 - c. will be changed at least every 60 days;
 - d. will not be a word appearing in an English or foreign dictionary;
 - e. will not be stored in keyboard macros, script, or batch files;
 - f. will not consist of personal ID data or be easily guessable;
 - g. will not reuse the same password within a 180 day period;
 - h. will have cycled through 10 passwords before reuse.

9. Passphrases:

A passphrase is a string of words and characters that you type in to authenticate yourself. Passphrases differ from passwords only in length. Passwords are usually short - six to ten characters. Passphrases are usually much longer - up to 100 characters or more. A passphrase should be known only to you, long enough to be secure, hard to guess -- even by someone who knows you well, and easy for you to remember and type accurately. In addition to the restrictions for passwords listed previously, passphrases:

- a. will be a minimum of 20 characters in length (including spaces);
 - b. will be a minimum of 4 words;
 - c. will be at least 6 unique characters (characters with only 1 occurrence in passphrase);
 - d. will have at least one character from each of the three groups: MiXeD CaSe letters, numeric characters, punctuation and special characters;
 - e. will not reuse the same passphrase within a 2 year period;
 - f. will have cycled through 5 passphrases before reuse;
 - g. can not be cached.
10. Challenge anyone in your facility who does not have proper identification.

11. E-mail and other forms of electronic distribution will only be used for official purposes and will not be used to transmit the following information:
- a. U.S. Government or corporate credit card numbers;
 - b. Designated Sensitive Data;
 - c. Risk Assessments;
 - d. For Official Use Only information;
 - e. Privacy Act Data;
 - f. Proprietary Data;
 - g. Procurement Sensitive Data;
 - h. Source Evaluation Board (SEB) information;
 - i. Closed IONet IP Address(es) and local/remote workstation IP Address(es);
 - j. Port numbers;
 - k. Usernames, Passwords and Passphrases.
12. Tampering or reverse engineering of the IT resource is prohibited.
13. Any unauthorized penetration attempt, unauthorized system use, or virus activity will be reported to your supervisor, project manager, system administrator and IT Security Officer.
14. When access is no longer required to these IT resources, notify appropriate responsible parties and make no further attempt to access these resources.
15. Failure to adhere to these rules or subvert these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

Acknowledgement Statement

Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Section 799, Title 18, U.S. Code; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts, and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

Requester's Signature

Date Signed

Please Print

User's Full Name:	Phone Number:
Project or Mission:	
Employer/Affiliation/Organization/Code:	
Location or Address:	
Email Address:	
Supervisor or Project Manager:	Phone Number:
FQDN/IP Address(es):	
Level of Privilege: Mission Scheduler or Mission Manager	Citizenship of Requestor

Fax completed form to the WSC SN Database Manager: (505) 527-7233